Are Thermal Attacks Ubiquitous? When Non-Expert Attackers Use Off the shelf Thermal Cameras

Yasmeen Abdrabou
Yomna Abdelrahman
Bundeswehr University Munich
yabdrabou@acm.org
yomna.abdelrahman@unibw.de

Ahmed Ayman
Amr Elmougy
German University in Cairo
firstname.lastname@guc.edu.eg

Mohamed Khamis
University of Glasgow
mohamed.khamis@glasgow.ac.uk

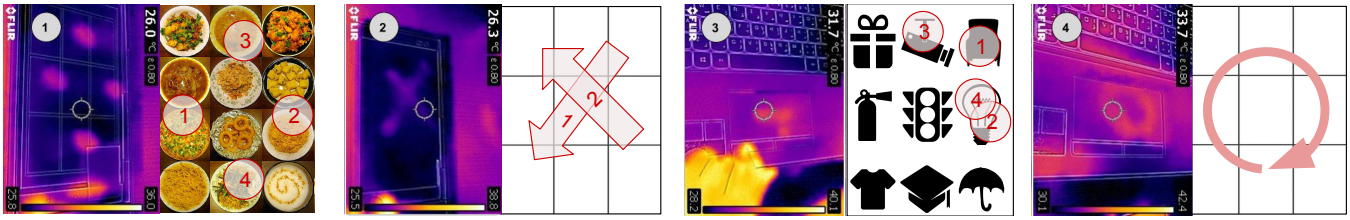


Figure 1: Thermal images of graphical passwords entered on a smartphone's touchscreen (1 and 2) and a laptop's touchpad (3 and 4) were visually inspected by participants, who recovered 60.65% of touch gestures (2 and 4), and 23.61% of touch taps (1 and 3). Attacks against touchscreens are more accurate (87.04% vs 56.02%). The red circles/arrows illustrate the user's input.

Abstract

Recent work showed that using image processing techniques on thermal images taken by high-end equipment reveals passwords entered on touchscreens and keyboards. In this paper, we investigate the susceptibility of common touch inputs to thermal attacks when non-expert attackers visually inspect thermal images. Using an off-the-shelf thermal camera, we collected thermal images of a smartphone's touchscreen and a laptop's touchpad after 25 participants had entered passwords using touch gestures and touch taps. We show that visual inspection of thermal images by 18 participants reveals the majority of passwords. Touch gestures are more vulnerable to thermal attacks (60.65% successful attacks) than touch taps (23.61%), and attacks against touchscreens are more accurate than on touchpads (87.04% vs 56.02%). We discuss how the affordability of thermal attacks and the nature of touch interactions make the threat ubiquitous, and the implications this has on security.

CCS Concepts

• **Human-centered computing** → **Human computer interaction (HCI)**; • **Security and privacy** → **Authentication**.

Keywords

Thermal Imaging, Security, Privacy, Graphical Authentication

ACM Reference Format:
Yasmeen Abdrabou, Yomna Abdelrahman, Ahmed Ayman, Amr Elmougy, and Mohamed Khamis. 2020. Are Thermal Attacks Ubiquitous? When Non-Expert Attackers Use Off the shelf Thermal Cameras. In *International Conference on Advanced Visual Interfaces (AVI '20), September 28-October 2, 2020, Salerno, Italy*. ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3399715.3399819

AVI '20, September 28-October 2, 2020, Salerno, Italy

1 Introduction

Recent work showed that thermal attacks are effective in retrieving passwords by using expensive thermal cameras [1] and/or employing automated image processing approaches [1, 18, 23]. To date, it is not well understood to what extent a non-expert with no technical skills can conduct thermal attacks using an off the shelf camera. If non-experts can perform thermal attacks without any technical background, then this means the majority of the population can perform the attack, making the threat ubiquitous. Compared to previously considered threats, studying threats by untrained attackers sheds light on a) how realistic the risk of thermal attacks is, and b) how ubiquitous thermal attacks can be.

We close this gap by investigating how well untrained attackers infer touch *taps* (Fig. 1.1 and 1.3) and touch *gestures* (Fig. 1.2 and 1.4) by visually inspecting thermal images. In a first study (N=25), we collected thermal images of *gestures* and *taps* resulting from authenticating using two graphical authentication schemes on a smartphone's *touchscreen* and a laptop's *touchpad*. In a second study, 18 new participants inspected the thermal images visually to infer the passwords. Inputs are correctly guessed 60.65% and 23.61% of the time in case of *gestures* and *taps* respectively. Guesses based on thermal attacks are fully correct at almost equal rates across *touchscreens* (43.06%) and *touchpads* (41.2%). More guesses against *touchscreens* (87.04%) are partially correct compared to *touchpads* (56.02%). Tapping is more secure on *touchpads* than on touchscreens, and touch gestures are more secure on touchscreens than on *touchpads*. We discuss how the nature of interactions and physical properties of interfaces contribute to the success of thermal attacks. Our results highlight that thermal attacks are becoming ubiquitous and have significant implications on touch-based authentication.

2 Background and Related Work

Users unlock their mobile devices around 40 times a day, thereby creating many occasions in which users are subject to side channel attacks, such as observation attacks [13], video attacks [33], smudge attacks [6], and thermal attacks [1]. While observation, video and smudge attacks were extensively researched in previous work [12, 26, 28, 29], thermal attacks are relatively under investigated.

In thermal attacks, thermal cameras capture heat traces left on interfaces after authentication [1, 23, 31]. When the user touches a surface, heat is transferred from the users' hand to the touched surfaces. This generates a temperature difference at the point of contact referred to as heat traces. Heat traces can be detected using thermal cameras. Mowery et al. [23] were among the first to explore thermal attacks by using an $18,000 thermal camera and an automated approach to find PINs on plastic ATM keypads. They found thermal attacks ineffective against metal keypads as they reflect heat signatures. Further research underlined the threat's significance on mobile authentication [1, 4]. Abdelrahman at al. [1] studied thermal attacks on PINs and Android Patterns on smartphone touchscreens. They found that password properties, such as duplicate digits in PINs and overlaps in Patterns, impact the attack's success. They also used a high end thermal camera and an image processing algorithm to detect passwords up to 30 seconds after authentication. Kaczmarek et al. [18] studied thermal attacks on external keyboards. Using an automated approach, their attacks could recover key presses up to 30 seconds after entry.

While prior work used expensive thermal cameras (e.g., $5,900–$18,000 [1, 23]), or automated approaches [1, 18, 21, 23, 31], we study thermal attacks where non-expert attackers visually inspect thermal images taken by an affordable (<$450) off-the-shelf thermal camera. This means that we consider a threat model that is more realistic, more likely to happen, and potentially more ubiquitous. In addition, we compare the thermal attack resistance of touch gestures and touch taps when entered on touchcsreens and touchpads.

3 Threat Model

In our threat model, the attacker waits until the victim authenticates on a laptop or a mobile device and then leaves it unattended. To ensure optimal but realistic attack conditions, the user does not interact after authenticating (e.g., quickly checking messages, emails, etc.) before temporarily leaving the device to attend to something else (e.g., get coffee). The attacker takes a thermal image of the interface and visually inspects it to guess the password.

4 Evaluation

Our evaluation entailed two phases: 1) dataset collection, and 2) thermal attack execution. Both complied with ethics and privacy regulations of the university in which they took place. Both study phases were designed as within-subjects experiments where all participants went through two independent variables.

IV1) Input Type: Gestures (Drawmetric) and Taps (Locimetric): We studied two input types: touch gestures and touch taps. Gestures are commonly used for drawmetric graphical passwords (aka recall authentication schemes) [8], such as Draw-A-Secret [17], Pass Shapes [30], and free form gestures [22, 32]. Gestures are sometimes also used for cued-recall schemes [26]. Recent research prototypes, such as SwiPIN [27], XSide [12] and CueAuth [20], also make use of touch gestures. Lock Patterns on Android is an example of a commercial adoption of authentication using touch gestures. On the other hand, taps are used for PINs, and for locimetric graphical passwords [5] where the user selects multiple points on one or more images. Examples include PassPoints [24], and CGP [14]. Windows 10's image password is a sample Locimetric scheme.

IV2) Input Interface: Touchscreen and Touchpad We compared a smartphone's gorilla glass touchscreen (touchscreen for short), and a laptop's capacitive touchpad (touchpad for short). Materials exhibit different thermal conductance [2], which means that touchscreens' resistance to thermal attacks (e.g., in [1, 4]) is not necessarily similar to that of touchpads.

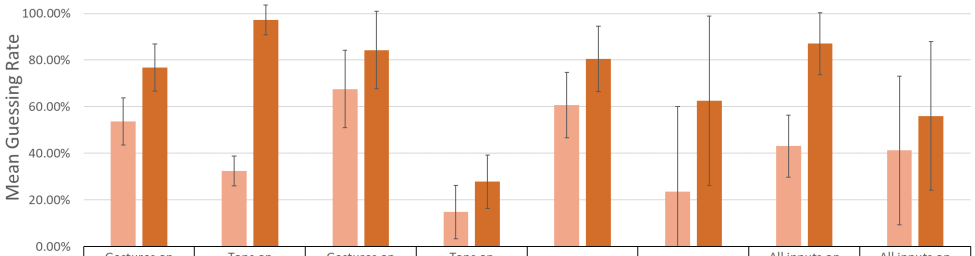
Implementation To collect input from participants, we implemented Android and Windows versions of drawmetric and locimetric schemes. The drawmetric scheme is similar to Draw-A-Secret [17] and allows participants to freely draw on the touchscreen and touchpad using touch gestures (Figures 1.2 and 1.4). While the locimetric one follows prior implementations of cued-recall passwords [3]. The scheme overlays a picture over a 3×3 grid on which the user has to tap some positions on the touchscreen, or navigate the pointer then tap using the touchpad (Figures 1.1 and 1.3).

4.1 Phase 1: Data Collection

To collect a dataset of thermal images to be used in the subsequent security study, we invited 25 participants (9 females) aged between 18 and 28 (Mean=22; SD=2.7) through university mailing lists.

4.1.1 Procedure The experiment was conducted in a temperature controlled room in our lab (24°C). Upon arrival, participants were explained the study and asked to sign a consent form and a demographics questionnaire. We recorded the participants' hand temperature, as well as that of the touchscreen and the touchpad. After introducing the two authentication schemes, we gave the participants 4 minutes to familiarize themselves with them. We then told the participants the password they had to enter one at a time according to a predefined list of passwords. We explain how we generated the list in the following section. The passwords in our list were illustrated on paper and handed to participants. To prevent heat traces of different entries from mixing up, participants waited for one minute before entering the following password to allow the older heat traces to fade. Each participant entered 24 different passwords (2 input interfaces × (6 drawmetric passwords + 6 locimetric passwords)). The order of conditions was counter balanced using Latin-Square. A thermal image of the interface was taken 4 seconds after completing the entry (see Figure 1) . We chose 4 seconds as our pilot tests using the Flir C2 Compact thermal camera showed that the heat traces fade away significantly after 4 seconds. We discarded the data of P19 because her hand temperature was too low (≈ 25°C) that few heat traces were visible due to cold fingertips.

4.1.2 Choice of Passwords To ensure ecological validity, our choice of passwords to be entered by participants is inspired by common passwords as identified in prior work. For drawmetric passwords, half of the passwords in the list were letter-shaped gestures (e.g., gestures that look like T, S, and Z), while the other half were shapes such as squares, circles and stars. This was motivated by Yulong et al.'s [32] finding that users tend to use letters and shapes as



	Gestures on Smartphone's Touchscreen	Taps on Smartphone's Touchscreen	Gestures on Laptop's Touchpad	Taps on Laptop's Touchpad	Gestures on both Interfaces	Taps on both Interfaces	All inputs on Smartphone's Touchscreen	All inputs on Laptop's Touchpad
Correct	53.70%	32.41%	67.59%	14.81%	60.65%	23.61%	43.06%	41.20%
Partially Correct	76.85%	97.22%	84.26%	27.78%	80.56%	62.50%	87.04%	56.02%

Figure 2: Attack success rates for the different input schemes and input interfaces. Taps are significantly more secure against thermal attacks compared to touch gestures. Tapping on a laptop's touchpad is significantly more secure than tapping on a smartphone's touchscreen, and touch gestures are significantly more secure on touchscreens than on touchpads.

free-form recall graphical passwords. Our choice of locimetric passwords was motivated by common distributions of password points according to prior field studies on cued-recall passwords [3].

4.1.3 Apparatus We used a Flir C2 Compact [**?**] Camera (80 px × 60 px), which is a low-cost off the shelf thermal camera (<$450). The camera was mounted on a 25 cm high tripod placed 30 cm away from the interface. Passwords were entered on a Lenovo Tango Phab 2 Pro smartphone with a gorilla glass screen (1440 px × 2560 px) pixels, and a Lenovo z50 Laptop (1920 px × 1080 px).

4.2 Phase 2: Analyzing Thermal Attacks

To simulate thermal attacks against the collected images, we invited participants to visually inspect and infer the passwords. We recruited 18 new participants (8 females) aged between 18 and 54 (Mean=26; SD=11) through mailing lists to take the role of attackers. We considered two dependent variables to evaluate attacks:

DV1 Correct Guess: an attack is considered successful if the whole guess is entry correctly. For gestures, a correct guess means successfully uncovering the shape and the direction of the input. For taps, it means successfully uncovering the positions and the order of input.

DV2 Partially Correct Guess: this refers to uncovering the *shape* but not the direction in case of touch gestures, or the *positions* of input and not their order in case of touch taps.

4.2.1 Procedure We first explained how the authentication schemes work and how to provide input. We then showed the participants a sample thermal image for each condition to explain how thermal attacks take place. We also explained that heat traces fade over time and this could be used to determine the order and direction of entry. After filling a consent form and a demographics questionnaire, participants were then provided with the thermal images one after another, and a pen and paper to write down their guesses. In total, each participant performed 24 attacks (6 attacks × 2 input types × 2 input interfaces). Participants made up to three guesses per attack; only the best of the three was considered for analysis. For each guess, we logged the guessed password, and the guessed direction/order of input. Participants were not told whether their guesses are correct until the end of the study to avoid any potential biases. The order of conditions in which we presented the thermal images was counter balanced using Latin square. To encourage participants, we created a scoring mechanism and a scoreboard. Participants received two points for each Correct Guess (DV1), and one point for each Partially Correct Guess (DV2). Scores were also based on the best of the three guesses.

4.3 Limitations

Participants with high hand temperatures left more visible heat traces (e.g., P4's hand temperature was 45°C, while P19's was 25°C). This is mitigated by following a within-subjects experiment design, which controls individual differences [16]. Nevertheless, we expect relative results to remain generalizable. For example, we expect gestures to remain more vulnerable compared to taps, and a higher accuracy of attacks against touchscreens compared to touchpads.

5 Results

5.1 Effect on Correct Guesses

A two-way repeated measures ANOVA revealed significant main effects for input type $F_{1,17} = 42.43$, $p < 0.001$, but not for input interface ($p > 0.05$) on Correct Guesses. We found a significant two-way interaction effect between input type and input interface $F_{1,17} = 11.642$, $p < 0.005$. This means that Correct Guesses depend on a) input type and b) combination of input type and input interface. Thus, we carried out additional one-way ANOVA tests.

5.1.1 Input Type effect on Correct Guesses against Touchscreens For touchscreens, a one-way ANOVA $F_{1,17} = 6.276$, $p < 0.05$ showed that correct guesses are significantly impacted by the input type. Post hoc analysis using Bonferroni-corrected t-tests indicated that attacks against touch gestures entered on touchscreens ($M = 53.7\%$, $SD = 17.67\%$) result in significantly more correct guesses ($p < 0.001$) than attacks against taps ($M = 32.41\%$, $SD = 25.23\%$).

5.1.2 Input Type effect on Correct Guesses against Touchpads For touchpads, a one-way ANOVA $F_{1,17} = 79.7$, $p < 0.001$ showed that correct guesses are significantly impacted by input type. Post hoc analysis using Bonferroni-corrected t-tests indicated that attacks against touch gestures entered on touchpads ($M = 67.59\%$, $SD = 20.19\%$) result in significantly more correct guesses ($p < 0.001$) than attacks against taps ($M = 14.81\%$, $SD = 13.87\%$).

5.2 Effect on Partially Correct Guesses

A two-way repeated measures ANOVA revealed significant main effects for input type $F_{1,17} = 44.677$, $p < 0.001$, and input interface

$F_{1,17} = 154.082$, $p < 0.001$ on part. corr. guesses. We found a significant two-way interaction effect between input type and input interface $F_{1,17} = 219.68$, $p < 0.001$. This means that part. corr. guesses depend on a) input type, b) input interface, and c) the combination of both. To distinguish the impact of input type from that of input interface, we carried out additional one-way ANOVAs.

5.2.1 Input Type effect on Part. Corr. Guesses on Touchscreens In case of touchscreens, a one-way ANOVA $F_{1,17} = 51.605$, $p < 0.001$ showed that part. corr. guesses are significantly impacted by input type. Post hoc analysis using Bonferroni-corrected t-tests indicated that attacks against gestures ($M = 76.85\%$, $SD = 10.13\%$) result in significantly more part. corr. guesses ($p < 0.001$) compared to taps ($M = 97.22\%$, $SD = 6.39\%$).

5.2.2 Input Type effect on Part. Corr. Guesses on Touchpads For touchpads, a one-way ANOVA $F_{1,17} = 160.827$, $p < 0.001$ showed part. corr. guesses are significantly impacted by input type. Post hoc analysis indicated attacks against gestures ($M = 87.26\%$, $SD = 16.64\%$) have significantly more part. corr. guesses ($p < 0.001$) than taps ($M = 27.78\%$, $SD = 11.43\%$).

5.3 Summary of the Results

The results (summarized in Figure 2) indicate that in terms of security against thermal attacks, a) tapping is significantly more secure than touch gestures, b) touch gestures are significantly more secure when entered on touchscreens than on touchpads, and c) tapping is significantly more secure on touchpads than on touchscreens.

6 Discussion and Future Work

Results show the possibility to use a low-cost thermal camera to conduct thermal attacks by visually inspecting the thermal images.

Lesson 1: Touch input is Highly Vulnerable to Thermal Attacks, but Taps are Relatively More Secure than Gestures. The results indicate that both tapping and touch gestures are highly vulnerable to thermal attacks. We recommend using taps rather than gestures as the latter are more vulnerable. This is inline with previous work in which Android Patterns, which require touch gestures, are inferred using automatic approaches and high end cameras. Although our evaluation of taps was performed on a graphical locimetric password scheme, these outcomes are also relevant for passwords that require tapping, such as PINs.

Our results compare types of touch input and not types of graphical authentication schemes. While we followed the most common implementations of drawmetric and locimetric schemes [3, 17, 26], this does not generalize to all graphical passwords. The security of graphical passwords can be improved by, for example, using contactless input for, such as eye gaze or mid-air gestures. Indeed, one direction to address thermal attacks is to employ schemes that use modalities that do not leave heat traces [9, 10, 14, 19]. An alternative could be to use cue-based authentication where the user's input depends on system cues [7, 20, 25, 27]. While cue-based authentication leaves heat traces, the dependency on cues requires adversaries to learn which cues the user responded to when providing input, thereby complicating attacks. Another direction is to employ biometric schemes that are usually more usable, such as keystroke dynamics [11, 15], and facial or fingerprint recognition. Future work should study how resilient biometrics are against thermal attacks, and improve their usability to maximize adoption.

Lesson 2: Touchpads are more Secure against Thermal Attacks. While successful attacks against touchscreens (43.06%) are as high as touchpads (41.2%), guesses are significantly more accurate on touchscreens (87.04% partially correct guesses) than touchpads (56.02% partially correct guesses). This means attacks are less effective when using touchpads of laptops.

This is due to the nature of interaction on touchpads compared to touchscreens; to authenticate using a touchscreen, the user's finger touches the screen at the first input position, while on touchpads the user needs to navigate their mouse pointer to reach the first input position. The interactions that move the mouse pointer create additional heat traces that blend into those resulting from authentication. Therefore, the threat is relatively lower on touchpads.

Thermal Attacks are Becoming Ubiquitous and can be Performed by Anyone Overall, the results indicate that both taps and gestures are highly vulnerable to thermal attacks. Previous work employed image processing to analyze thermal images and infer entered passwords using high end thermal cameras that cost more than $5,900 [1, 23]. Our work shows that attackers can achieve an alarming success rate by visually inspecting thermal images taken by an off the shelf thermal camera that costs less than $450. These results underline how critical and timely it is to address thermal attacks. Thermal cameras will continue to become cheaper and accessible to a many potential adversaries who could use them maliciously without any technical expertise.

7 Conclusion

We evaluated the effectiveness of thermal attacks by non-expert attackers using an off the shelf thermal camera. We collected a dataset of thermal images of a smartphone's touchscreen and a laptop's touchpad after participants entered graphical passwords using touch taps and gestures. In a second study, 18 participants visually inspected the thermal images to infer the passwords. They recovered 60.65% of touch gestures and 23.61% of touch taps. Attacks against touchscreens and touchpads are almost equally successful, but are more accurate on touchscreens. These results highlight that thermal attacks are likely to become ubiquitous, especially with the affordability of thermal cameras and the feasibility of attacks without any image processing as done in previous work [1, 23]. We discussed how the user's behavior and the physical properties of the two studied interfaces impact the success of thermal attacks, and future work directions to counter the ubiquity of thermal attacks.

Acknowledgments

This work was supported by the Royal Society of Edinburgh (RSE award no. 65040), the German Research Foundation (DFG), Grant No. 316457582 and AL 1899/2-1, and the Studienstiftung des deutschen Volkes ("German Academic Scholarship Foundation"). Figure 1.1 by pallavi_damera on Flickr https://www.flickr.com/photos/pallavi_damera/2536005489 (CC BY 2.0)

References

[1] Yomna Abdelrahman, Mohamed Khamis, Stefan Schneegass, and Florian Alt. 2017. Stay Cool! Understanding Thermal Attacks on Mobile-based User Authentication *(CHI '17)*. ACM, New York, NY, USA, 3751–3763. https://doi.org/10.1145/3025453.3025461

[2] Yomna Abdelrahman, Alireza Sahami Shirazi, Niels Henze, and Albrecht Schmidt. 2015. Investigation of Material Properties for Thermal Imaging-Based Interaction *(CHI '15)*. ACM, New York, NY, USA, 15–18. https://doi.org/10.1145/2702123.2702290

[3] Florian Alt, Stefan Schneegass, Alireza Sahami Shirazi, Mariam Hassib, and Andreas Bulling. 2015. Graphical Passwords in the Wild: Understanding How Users Choose Pictures and Passwords in Image-based Authentication Schemes *(MobileHCI '15)*. ACM, New York, NY, USA, 316–322. https://doi.org/10.1145/2785830.2785882

[4] Panagiotis Andriotis, Theo Tryfonas, George Oikonomou, and Can Yildiz. 2013. A pilot study on the security of pattern screen-lock methods and soft side channel attacks. In *Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks*. ACM, 1–6.

[5] Antonella De Angeli, Lynne Coventry, Graham Johnson, and Karen Renaud. 2005. Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems. *International Journal of Human-Computer Studies* 63, 1 (2005), 128 – 152. https://doi.org/10.1016/j.ijhcs.2005.04.020 HCI research in privacy and security.

[6] Adam J. Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M. Smith. 2010. Smudge Attacks on Smartphone Touch Screens. (2010), 1–7. http://dl.acm.org/citation.cfm?id=1925004.1925009

[7] Andrea Bianchi, Ian Oakley, and Dong Soo Kwon. 2012. Counting Clicks and Beeps: Exploring Numerosity Based Haptic and Audio PIN Entry. *Interact. Comput.* 24, 5 (Sept. 2012), 409–422. https://doi.org/10.1016/j.intcom.2012.06.005

[8] Robert Biddle, Sonia Chiasson, and P.C. Van Oorschot. 2012. Graphical Passwords: Learning from the First Twelve Years. *ACM Comput. Surv.* 44, 4, Article 19 (Sept. 2012), 41 pages. https://doi.org/10.1145/2333112.2333114

[9] Andreas Bulling, Florian Alt, and Albrecht Schmidt. 2012. Increasing the security of gaze-based cued-recall graphical passwords using saliency masks. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 3011–3020.

[10] Alexander De Luca, Martin Denzel, and Heinrich Hussmann. 2009. Look into My Eyes!: Can You Guess My Password? *(SOUPS '09)*. ACM, New York, NY, USA, Article 7, 12 pages. https://doi.org/10.1145/1572532.1572542

[11] Alexander De Luca, Alina Hang, Frederik Brudy, Christian Lindner, and Heinrich Hussmann. 2012. Touch Me Once and I Know It's You!: Implicit Authentication Based on Touch Screen Patterns *(CHI '12)*. ACM, New York, NY, USA, 987–996. https://doi.org/10.1145/2207676.2208544

[12] Alexander De Luca, Marian Harbach, Emanuel von Zezschwitz, Max-Emanuel Maurer, Bernhard Ewald Slawik, Heinrich Hussmann, and Matthew Smith. 2014. Now You See Me, Now You Don'T: Protecting Smartphone Authentication from Shoulder Surfers *(CHI '14)*. ACM, New York, NY, USA, 2937–2946. https://doi.org/10.1145/2556288.2557097

[13] Malin Eiband, Mohamed Khamis, Emanuel von Zezschwitz, Heinrich Hussmann, and Florian Alt. 2017. Understanding Shoulder Surfing in the Wild: Stories from Users and Observers *(CHI '17)*. ACM, New York, NY, USA, 4254–4265. https://doi.org/10.1145/3025453.3025636

[14] Alain Forget, Sonia Chiasson, and Robert Biddle. 2010. Shoulder-surfing resistance with eye-gaze entry in cued-recall graphical passwords. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 1107–1110.

[15] Mario Frank, Ralf Biedert, Eugene Ma, Ivan Martinovic, and Dawn Song. 2013. Touchalytics: On the Applicability of Touchscreen Input As a Behavioral Biometric for Continuous Authentication. *Trans. Info. For. Sec.* 8, 1 (Jan. 2013), 136–148. https://doi.org/10.1109/TIFS.2012.2225048

[16] Anthony G. Greenwald. 1976. Within-subjects designs: To use or not to use? *Psychological Bulletin* 83, 2 (1976), 314–320. https://doi.org/10.1037/0033-2909.83.2.314

[17] Ian Jermyn, Alain Mayer, Fabian Monrose, Michael K. Reiter, and Aviel D. Rubin. 1999. The Design and Analysis of Graphical Passwords. In *Proceedings of the 8th Conference on USENIX Security Symposium - Volume 8*. USENIX Association, Berkeley, CA, USA, 1–1. http://dl.acm.org/citation.cfm?id=1251421.1251422

[18] Tyler Kaczmarek, Ercan Ozturk, and Gene Tsudik. 2019. Thermanator: Thermal Residue-Based Post Factum Attacks on Keyboard Data Entry *(Asia CCS '19)*. ACM, New York, NY, USA, 586–593. https://doi.org/10.1145/3321705.3329846

[19] Christina Katsini, Yasmeen Abdrabou, George Raptis, Mohamed Khamis, and Florian Alt. 2020. The Role of Eye Gaze in Security and Privacy Applications: Survey and Future HCI Research Directions. *(CHI '20)*. ACM, New York, NY, USA.

[20] Mohamed Khamis, Ludwig Trotter, Ville Mäkelä, Emanuel von Zezschwitz, Jens Le, Andreas Bulling, and Florian Alt. 2018. CueAuth: Comparing Touch, Mid-Air Gestures, and Gaze for Cue-based Authentication on Situated Displays. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2, 4, Article 174 (Dec. 2018), 21 pages. https://doi.org/10.1145/3287052

[21] Duo Li, Xiao-Ping Zhang, Menghan Hu, Guangtao Zhai, and Xiaokang Yang. 2019. Physical Password Breaking via Thermal Sequence Analysis. *IEEE Transactions on Information Forensics and Security* 14, 5 (May 2019), 1142–1154. https://doi.org/10.1109/TIFS.2018.2868219

[22] Can Liu, Gradeigh D. Clark, and Janne Lindqvist. 2017. Where Usability and Security Go Hand-in-Hand: Robust Gesture-Based Authentication for Mobile Systems *(CHI '17)*. ACM, New York, NY, USA, 374–386. https://doi.org/10.1145/3025453.3025879

[23] Keaton Mowery, Sarah Meiklejohn, and Stefan Savage. 2011. Heat of the Moment: Characterizing the Efficacy of Thermal Camera-based Attacks *(WOOT'11)*. USENIX Association, Berkeley, CA, USA, 6–6. http://dl.acm.org/citation.cfm?id=2028052.2028058

[24] Deholo Nali and Julie Thorpe. 2004. Analyzing user choice in graphical passwords. *School of Computer Science, Carleton University, Tech. Rep. TR-04-01* (2004).

[25] Volker Roth, Kai Richter, and Rene Freidinger. 2004. A PIN-entry Method Resilient Against Shoulder Surfing *(CCS '04)*. ACM, 236–245. https://doi.org/10.1145/1030083.1030116

[26] Stefan Schneegass, Frank Steimle, Andreas Bulling, Florian Alt, and Albrecht Schmidt. 2014. SmudgeSafe: Geometric Image Transformations for Smudge-resistant User Authentication *(UbiComp '14)*. ACM, New York, NY, USA, 775–786. https://doi.org/10.1145/2632048.2636090

[27] Emanuel von Zezschwitz, Alexander De Luca, Bruno Brunkow, and Heinrich Hussmann. 2015. SwiPIN: Fast and Secure PIN-Entry on Smartphones *(CHI '15)*. ACM, New York, NY, USA, 1403–1406. https://doi.org/10.1145/2702123.2702212

[28] Emanuel von Zezschwitz, Alexander De Luca, Philipp Janssen, and Heinrich Hussmann. 2015. Easy to Draw, but Hard to Trace?: On the Observability of Grid-based (Un)Lock Patterns *(CHI '15)*. ACM, New York, NY, USA, 2339–2342. https://doi.org/10.1145/2702123.2702202

[29] Emanuel von Zezschwitz, Anton Koslow, Alexander De Luca, and Heinrich Hussmann. 2013. Making Graphic-based Authentication Secure Against Smudge Attacks *(IUI '13)*. ACM, New York, NY, USA, 277–286. https://doi.org/10.1145/2449396.2449432

[30] Roman Weiss and Alexander De Luca. 2008. PassShapes: utilizing stroke based authentication to increase password memorability. In *Proceedings of the 5th Nordic conference on Human-computer interaction: building bridges*. ACM, 383–392.

[31] Wojciech Wodo and Lucjan Hanzlik. 2016. Thermal Imaging Attacks on Keypad Security Systems *(ICETE 2016)*. SCITEPRESS - Science and Technology Publications, Lda, Portugal, 458–464. https://doi.org/10.5220/0005998404580464

[32] Yulong Yang, Gradeigh D. Clark, Janne Lindqvist, and Antti Oulasvirta. 2016. Free-Form Gesture Authentication in the Wild *(CHI '16)*. ACM, New York, NY, USA, 3722–3735. https://doi.org/10.1145/2858036.2858270

[33] Guixin Ye, Zhanyong Tang, Dingyi Fang, Xiaojiang Chen, Willy Wolff, Adam J. Aviv, and Zheng Wang. 2018. A Video-based Attack for Android Pattern Lock. *ACM Trans. Priv. Secur.* 21, 4, Article 19 (July 2018), 31 pages. https://doi.org/10.1145/3230740